BEVEILIGING

SCENARIO 11: firewall

BEDOELING: Binnenkomend én uitgaand verkeer op elke pc controleren.
SITUATIE: Momenteel draait op enkele pc's Windows Firewall, als onderdeel van Service Pack 2, maar dat vindt pa onvoldoende.
INGREDIËNTEN: Windows XP (met Service Pack 2); (gratis) ZoneAlarm.

Je zou kunnen denken dat je pc's ook zonder firewall genoeg afgeschermd zijn. Ze krijgen immers van de router een intern ip-adres dat van buitenaf niet rechtstreeks te benaderen is. Vraagt een van deze pc's een internetverbinding aan, dan noteert de router het interne ip-adres van die pc, en stuurt dat verzoek vervolgens met éigen ip-adres het wereldwijde web op. Zodra de router een reactie op dat verzoek ontvangt, zoekt die snel op welke pc dat had aangevraagd en stuurt hij die reactie braafjes door naar dat interne toestel. Krijgt de router data binnen die geen reactie zijn op een specifiek verzoek van een van de achterliggende pc's, dan negeert hij die zonder meer.
Dat geeft weliswaar al een zekere veiligheid, maar we raden toch aan om op elke pc ook een degelijke firewall te installeren. In Clickx 112 somden we in de rubriek 'Haal meer uit je breedbandverbinding' al een aantal voordelen op. Nu levert Windows met Service Pack 2 wel al een deftige firewall af, maar jammer genoeg controleert die vooralsnog enkel het binnenkomende verkeer. Verkeer dat naar buiten gaat, wordt niet nagekeken. Precies daarom kijk je beter uit naar een krachtigere firewall. Gratis exemplaren worden steeds zeldzamer, maar eentje is nog stevig overeind gebleven: ZoneAlarm...



Windows Firewall erkent zijn meerdere...

STAP 1 / INSTALLATIE & BASISCONFIGURATIE

Download de gratis versie van ZoneAlarm op **www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp**. Start de installatie door het gedownloade bestand uit te voeren. Is je Windows Firewall nog actief, dan krijg je op een bepaald moment een waarschuwing: kies dan voor **Blokkering opheffen**. Meteen na de installatie mag je ZoneAlarm activeren door op de knop **Yes** te drukken. Maak vervolgens duidelijk dat je enkel in de gratis versie geïnteresseerd bent door **Select ZoneAlarm** aan te stippen. Bevestig met **Finish**. Er verschijnt nu een nieuw dialoogvenster waarin je tweemaal op **Next** drukt (laat de standaardinstellingen ongemoeid), en dat je vervolgens afsluit met **Done**. Herstart je computer, en je zal merken dat ZoneAlarm in het Beveiligingscentrum van XP de bovenhand heeft genomen op Windows Firewall (zie afbeelding 1).

Network Log
View network activity and security logs.

```
woensdag 1 februari 2006 16:41:08 DHCP:renew
woensdag 1 februari 2006 16:41:08 DHCP:ack(DOL=4841,T1=2420,T2=2480)
woensdag 1 februari 2006 16:43:21 Unrecognized attempt blocked from
66.249.93.99:80 to TCP port 2572
woensdag 1 februari 2006 16:43:22 Unrecognized attempt blocked from
66.249.93.104:80 to TCP port 2568
woensdag 1 februari 2006 16:43:22 Unrecognized attempt blocked from
66.249.93.104:80 to TCP port 2562
woensdag 1 februari 2006 16:43:22 Unrecognized attempt blocked from
```

Save Clear Refresh

De router houdt vaak erg beperkte veiligheidslogs bij.



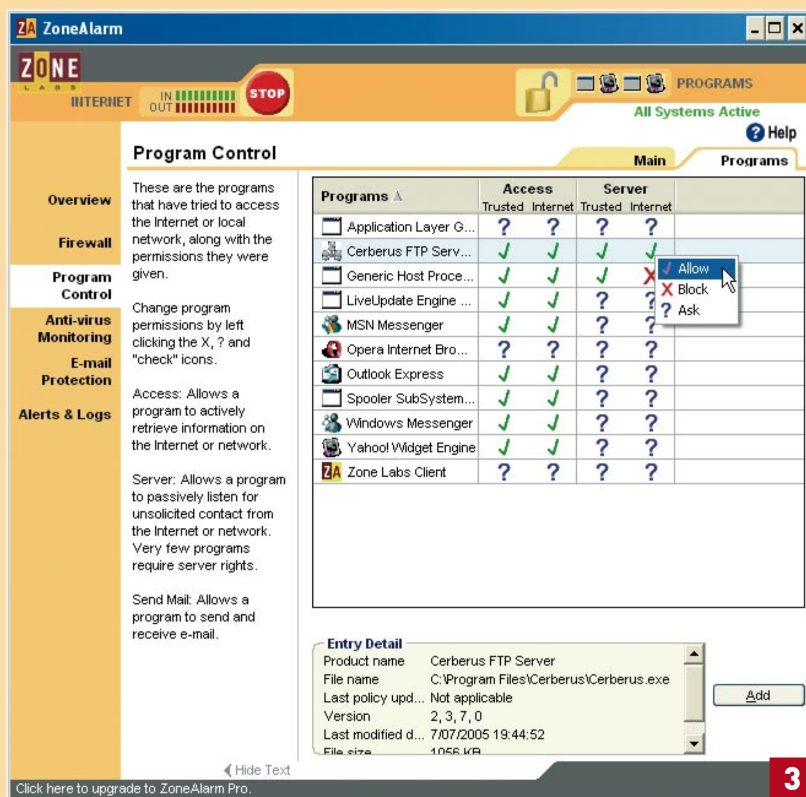
Laat je niet door elk alarm uit het lood slaan!

STAP 2 / ALARM!

Kort na de herstart trakteert ZoneAlarm je wellicht al op een paar alarmerende venstertjes. De kans is groot dat het gewoon om bonafide programma's gaat die een internetverbinding zoeken – maar lees er toch maar grondig de informatie in het venster op na. Mogelijk brengt de knop **More info** meer duidelijkheid (zie afbeelding 2). Wil je een bepaalde applicatie voor eens en voor altijd toelaten, zet dan eerst een vinkje naast **Remember this setting** en druk daarna op de knop **Allow**. Een twijfelgeval trakteer je via de knop **Deny** maar beter op een (definitief) 'njet'. Installeer je nadien een nieuwe toepassing die contact zoekt met het internet, dan zal ZoneAlarm je hiervan op dezelfde manier op de hoogte brengen.

STAP 3 / BEHEERMODULE

Uiteraard kan je op elk moment de instellingen van ZoneAlarm nog bijschaven én ook in alarmberichten en logboeken snuisteren. Dat gebeurt via een beheermodule die je opent via een dubbelklik op het ZoneAlarm-icoontje in de Windows-taakbalk. Wil je een overzicht van welke programma's welke toelatingen hebben gekregen, dan klik je links **Program Control** aan, en open je vervolgens rechtsboven het tabblad **Programs**. In de eerste kolom zie je dan alle toepassingen die al een verbinding hebben willen leggen met je eigen netwerk (**Trusted**) of met het internet. De tweede kolom toont je of programma's zelf informatie van het netwerk of van het internet mogen ophalen, en in de derde kolom lees je of applicaties mogen reageren op ongevraagde verzoeken van het netwerk of van het internet. Een vinkje betekent 'ja', een kruisje 'neen'. Bij een vraagteken zal ZoneAlarm telkens expliciet naar je toelating vragen. Door deze icoontjes aan te klikken, kan je de toelating aanpassen (zie afbeelding 3).



Je kan ZoneAlarm altijd nog herconfigureren.

SCENARIO 12: draadloos netwerk

BEDOELING: Draadloos netwerk afsluiten voor onbevoegden (bijvoorbeeld de buren).
SITUATIE: Het draadloze netwerk is momenteel nog totaal onbeveiligd, en dat lijkt toch niet zo'n goed idee.
INGREDIËNTEN: Windows XP, software van draadloos toegangspunt (router).

STAP 1 / STANDAARDAANPASSINGEN

In stap 1 van scenario 2 hebben we de beveiliging van ons draadloos toegangspunt voorlopig gelaten voor wat ze is. Hoog tijd om daar verandering in te brengen. We willen namelijk niet dat buren met hun netwerkadapters al dan niet gewild gegevens uit ons netwerkje oppikken, of downloads starten! Je kan alvast beginnen met het moeilijker te maken voor potentiële pottenkijkers. Begin met het standaardwachtwoord van je toegangspunt te wijzigen in een steviger exemplaar, en wijzig meteen ook de standaardnaam van je draadloze netwerk – het zogenoemde SSID (Service Set Identifier). Deze naam wordt door de toegangspunten meestal automatisch over het netwerk verspreid (broadcast SSID). Eventueel kan je deze optie uitschakelen. Hou er wel rekening mee dat netwerkadapters het draadloze netwerk dan niet meer automatisch kunnen vinden; je zal het SSID eigenhandig moeten intikken.
Als je altijd van dezelfde netwerkadapters gebruik maakt, kan je verder overwegen het zogenoemde *mac-adres* van die adapters in het configuratiescherm van je draadloos toegangspunt op te nemen. Op die manier ontneem je andere adapters de mogelijkheid zich op je WLAN aan te sluiten – hoewel ervaren *wardrivers* zo'n beveiliging snel weten te omzeilen. Het mac-adres van je draadloze adapter vis je zo uit: tik 'cmd' in bij **Uitvoeren**, en bevestig met **OK**. Achter de opdrachtprompt voer je de opdracht 'ipconfig /all' uit (bevestig met **Enter**). Spoor je draadloze verbinding op en noteer de combinatie achter **Fysiek adres**. Dat is het gezochte mac-adres.



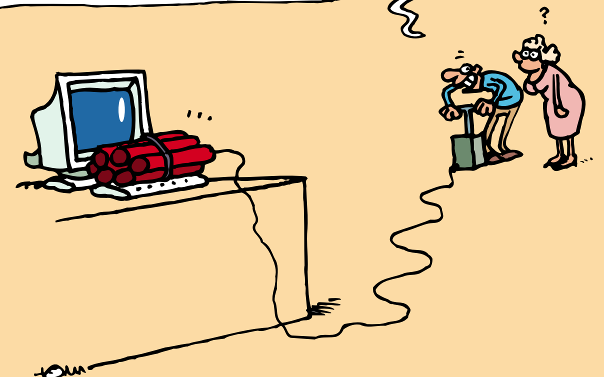
In het configuratiemenu van je router kan je al heel wat instellingen wijzigen die je netwerk beter beveiligen.



Je draadloze netwerk is pas veilig na encryptie met WPA.

STAP2 / TOEGANGSPUNT VERSLEUTELEN

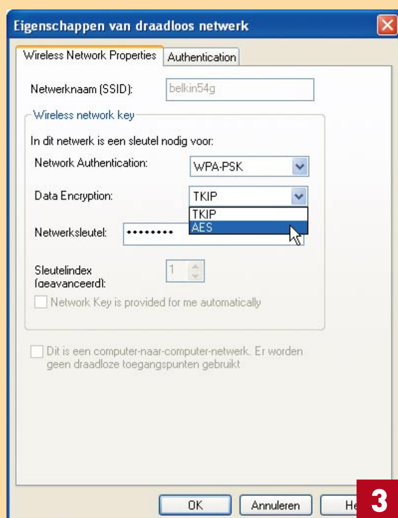
Zonder twijfel de belangrijkste vorm van beveiliging is het activeren van encryptie: alle gegevens circuleren dan versleuteld over het WLAN. Er zijn momenteel twee encryptiemethodes in gebruik: WEP (Wired Equivalent Privacy) en WPA (Wifi Protected Access). Van deze laatste bestaat intussen ook al een opvolger: WPA2. Heel wat toegangspunten bieden beide methodes aan, en in dat geval kies je zonder meer voor WPA, omdat deze techniek nóg veiliger is. Voorwaarde is natuurlijk wel dat ook al je draadloze adapters hiermee overweg kunnen – mogelijk pas na een *firmware*-upgrade. Deze encryptie activeer je vervolgens op je toegangspunt. Tik in je browser het interne ip-adres van je toegangspunt in. Ergens in het configuratievenster tref je zeker een optie aan die bijvoorbeeld naar de naam **Security** luistert. Kies hier **WPA**, en meer



bepaald de versie **PSK** die geen speciale server behoeft. PSK staat voor Pre-Shared Key en kan je in feite als een wachtwoord beschouwen. De meest frequente encryptietechniek is TKIP, maar als je netwerkadapters dat ondersteunen, kan je hier ook het nóg veiligere **AES** aanstippen. Tik een stevig wachtwoord in en bevestig (zie afbeelding 2). Herstart desnoods het toegangspunt.

STAP 3 / ADAPTERS HERCONFIGUREREN

Natuurlijk moet je elke WiFi-adapter nog afstemmen op de beveiliging die je in het toegangspunt hebt geactiveerd. Dat kan via de softwaretool die bij je adapter is geleverd, maar het gaat net zo goed met de tool die in Windows XP ingebouwd is. Om hiermee te werken, moet je de andere tool wellicht wel eerst duidelijk maken dat je de WiFi-configuratie aan XP overlaat. Open vervolgens het **Configuratiescherm** en kies **Netwerk- en Internet-verbindingen**, gevolgd door **Netwerkverbindingen.** Klik met de rechtermuisknop op de draadloze netwerkverbinding en kies **Eigenschappen.** Open het tabblad **Draadloze netwerken** en zorg dat de optie **Draadloos netwerk automatisch configureren** aangestipt is. Tref je hier nog geen beschikbare netwerken aan, druk dan op de knop **Draadloze netwerken** en vervolgens op **Verbinding maken** – in het andere geval selecteer je het gewenste netwerk bij **Voorkeursnetwerken** en druk je op **Eigenschappen.** Nu kan je de encryptiemethode en de netwerksleutel intikken (tweemaal), waarna je je keuzes bevestigt (zie afbeelding 3). Even later kan je adapter weer vlotjes communiceren met het draadloze toegangspunt.



Geef je netwerkadapter(s) dezelfde beveiliging mee!

VAKTAAL | A - M | N - Z

FIRMWARE: Bijna elk stukje hardware bevat firmware. Dit is een 'intelligent' stuk software dat er voor zorgt dat je randapparatuur (cd-rom speler, mp3-speler, pda) correct opstart en alles doet wat het moet doen. Voor veel apparaten wordt er regelmatig nieuwe firmware uitgebracht om extra functies toe te voegen of mankementen te verbeteren.

MAC-ADRES: Media Access Control. Elke netwerkkaart (draadloos of niet) bevat een uniek mac-adres. Dit is een code waarmee de netwerkkaart door het netwerk herkend wordt.

WARDRIVER: Sinds de opkomst van WiFi zijn er heel wat draadloze netwerken beschikbaar. Ook thuis en op het werk zijn er steeds meer draadloze netwerken. Bij wardriving gaat iemand met een notebook of pda op pad om niet-beschermde draadloze netwerken te ontdekken. Hij kan dan surfen op andermans kosten en zelfs gedeelde bestanden inkijken.

SCENARIO 13: ouderlijke controle

BEDOELING: Een zekere mate van ouderlijke controle uitoefenen op het computer- en vooral op het internetgebruik van de kinderen.

SITUATIE: Pa wil het computergebruik van zijn zoon niet alleen monitoren, maar ook inperken.

INGREDIËNTEN: Windows XP, UltraVNC, eventueel een beveiligingssuite en/of specifieke software voor ouderlijk toezicht.

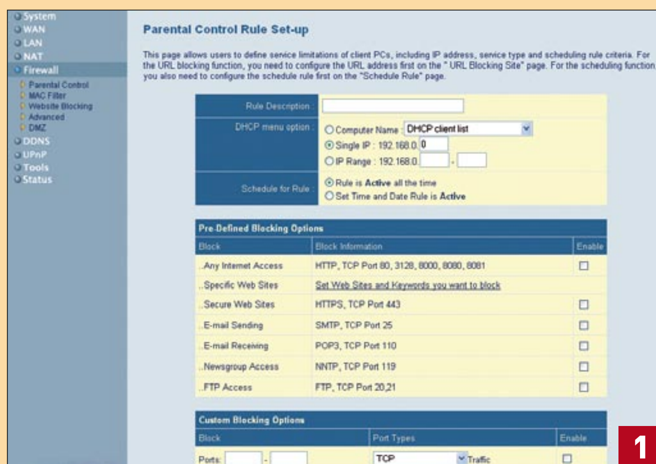
Onze redacteur heeft weliswaar al een vrij doortastende monitoringtool geïnstalleerd (zie UltraVNC in scenario 10), maar helemaal gelukkig is hij hier toch niet mee. Hij vindt het uiteindelijk toch een behoorlijke aanslag op de privacy. Hij gebruikt het dan ook zeer zelden, en communiceert zo'n controlesessie nadien ook telkens aan zijn zoon. Je kan natuurlijk ook (een combinatie van) minder doortastende middelen inzetten. Wij sommen de belangrijkste technieken even voor je op...

STAP 1 / ROUTER HOUDT JE KORT

Heel wat moderne routers hebben een ingebouwde firewallmodule voor ouderlijk toezicht (zie afbeelding 1). Het komt er gewoonlijk op neer dat je per (ip-adres van een) netwerktoestel kan instellen wannéér dat (niet) van bepaalde internetdiensten gebruik mag maken. Op die manier kan je bijvoorbeeld een tijdsklok zetten op het surfen, e-mailen, chatten en/of downloaden. Vaak kan je ook webadressen en zelfs sleutelwoorden intikken die de router vervolgens zal blokkeren. Een aantal routerproducenten zoals Linksys en Zyxell zijn zelfs scheep gegaan met online services voor ouderlijke controle, vergelijkbaar met de gespecialiseerde software die we in stap 3 vermelden. Deze online services zijn echter niet gratis.

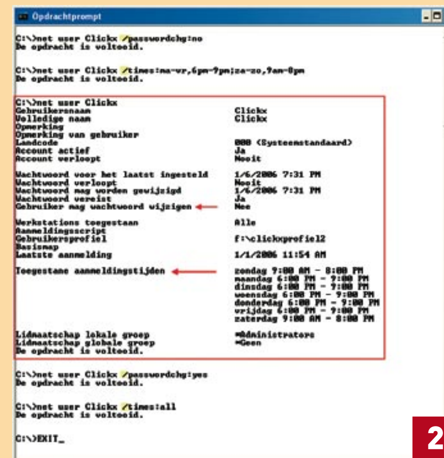
STAP 2 / WINDOWS XP HELPT OOK MEE

Ook zonder bijkomende software kan je al bepaalde beperkingen in Windows XP inbouwen. Je kan bijvoorbeeld vastleggen binnen welke tijdsspanne kindlief zich bij Windows mag aanmelden. Daarvoor start je de opdrachtprompt op. Dat doe je door bij **Uitvoeren** 'cmd' in te tikken, waarna je bevestigt met **OK**. Met de opdracht **net user gebruikersnaam /passwordchg:no** voorkom je dat de gebruiker zijn eigen inlogwachtwoord nog kan wijzigen – uiteraard vervang je **gebruikersnaam** door de juiste accountnaam van je kind. Met de parameter **/passwordchg:yes** laat je dat weer toe. Elke opdracht dien je wel met de **Enter**-toets te bevestigen. Vergeet absoluut niet het slash-teken in te tikken na de gebruikersnaam! Met een opdracht als **net user gebruikersnaam /times:ma-vr,6pm-9pm;za-zo,9am-8pm** beperk je de inlogtijden tot enkele uren per dag (in het weekend ben je iets soepeler). Gebruik je een Engelstalige Windows, pas dan de namen van de dagen aan. Vergeet ook hier de slash niet (zie afbeelding 2)!



1

De router houdt een (ouderlijk) oogje in het zeil...



2

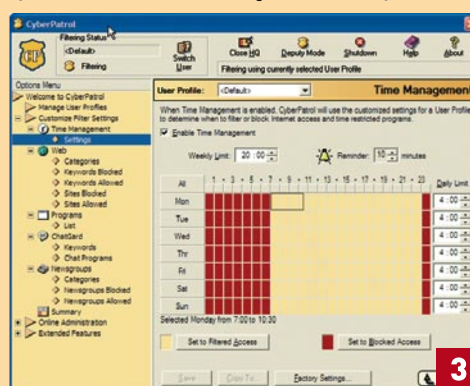
De aanmeldtijden kan je snel aan banden leggen.

STAP 3 / AAN DE SLAG MET GESPECIALISEERDE SOFTWARE

Je kan natuurlijk ook de hulp van extra software inroepen. Eigenlijk kan je hier twee wegen uit: een alomvattende beveiligingssuite, of een pakket dat in ouderlijk toezicht gespecialiseerd is.

McAfee Internet Security Suite 2006 **www.mcafee.com/nl** is een knappe beveiligingssuite met een flexibele inhoudsfilter die je per gebruiker kan instellen. Er is ook een optie om een tijdsslot in te stellen, zodat kindlief buiten de toegestane uren niet langer op internet geraakt. De suites Norton Internet Security 2006 **www.symantec.be/region/nl** en Panda Platinum 2006 Internet Security **www.pandasoftware.be** bevatten een vergelijkbare inhoudsfilter, maar ontberen een tijdsslot.

Verder zijn er nog een rist tools die zich puur toeleggen op ouderlijk toezicht. Het volgende trio behoort zonder twijfel tot de beste in hun soort: CyberPatrol **www.cyberpatrol.com** (zie afbeelding 3), CYBERsitter **www.cybersitter.com** en Net Nanny **www.netnanny.com**. Van elk van deze pakketten kan je een gratis proefversie downloaden. De prijs voor een jaarlijks abonnement schommelt telkens rond € 32.



3

CyberPatrol op patrouille...